UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC, *Plaintiff*, v. DMITRY STAROVIKOV; ALEXANDER FILIPPOV; Does 1–15, *Defendants*.	Civil Action No. 1:21-cv-10260-DLC

~~[PROPOSED]~~ PRELIMINARY INJUNCTION ORDER

Plaintiff Google LLC has filed a complaint for injunctive and other relief to stop Defendants Dmitry Starovikov and Alexander Filippov, and Does 1 through 15—through their participation in, and operation of, the Glupteba Enterprise—from continuing to control and operate a botnet of over a million devices, continuing to distribute malware to infect new devices, and continuing to carry out their criminal schemes.

Google filed a complaint alleging claims under: (1) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1962(c)–(d) (Count I); (2) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (Count II); (3) the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (Count III); (4) the Lanham Act (Count IV); (5) and common-law theories of unfair competition and unjust enrichment (Counts V–VI). ECF No. 5. On December 7, 2021, this Court issued a temporary restraining order

and order for Defendant to show cause why a preliminary injunction should not issue. ECF No. 8.

THE COURT HEREBY FINDS THAT:

Jurisdiction and Venue

1. This Court has federal-question jurisdiction over Google's claims under RICO, the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Lanham Act under 28 U.S.C. § 1331. This court also has jurisdiction over the Lanham Act and related state and common law unfair competition claims under 28 U.S.C. § 1338, and 15 U.S.C. § 1121. This court has supplemental jurisdiction over the state-law claims under 28 U.S.C. § 1367.

2. This Court has personal jurisdiction over the Defendants because:

a. The Defendants distribute malware to Google users in this district and within New York state;

b. The Defendants send commands to infected user computers in this district and within New York state to carry out their illicit schemes;

c. Google's complaint and moving papers demonstrate that the Defendants undertook these activities intentionally with knowledge that their actions would cause harm to users in New York and cause Google harm in New York. Google does business in New York and has done business in New York for many years.

3. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are not residents of the United States and may be sued in any judicial district. Venue is also proper in this judicial district under 28 U.S.C.

§ 1391(b) and 18 U.S.C. § 1965 because a substantial part of the events or omissions giving rise to Google's claims occurred in this judicial district, because a substantial part of the property that is the subject of Google's claims is situated in this judicial district, because a substantial part of the harm caused by Defendants has occurred in this judicial district, and because Defendants transact their affairs in this judicial district. Moreover, Defendants are subject to personal jurisdiction in this district and no other venue appears to be more appropriate.

4. The complaint pleads facts with the specificity required by the Federal Rules and states claims against Defendants for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1962(c)-(d) (Count I); the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (Count II), the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 (Count III), Lanham Act (Count IV), and unfair competition and unjust enrichment (Counts V–VI).

Preliminary Injunction Order Factors

The Court finds that Google has established each of the factors required for a preliminary injunction: (1) irreparable harm; (2) a likelihood of success on the merits or a substantial question as to the merits; (3) the balance of hardships tips in Google's favor; and (4) a preliminary injunction serves the public interest. *Benihana, Inc. v. Benihana of Tokyo, LLC*, 784 F.3d 887, 895 (2d Cir. 2015); *see also Sterling v. Deutsche Bank Nat'l Tr. Co. as Trustees for Femit Tr. 2006-FF6*, 368 F. Supp. 3d 723, 727 (S.D.N.Y. 2019) ("The standard[s] for granting a temporary restraining order and

a preliminary injunction pursuant to Rule 65 of the Federal Rules of [Civil] Procedure are identical.").

Irreparable Harm

5. Google has established that it will suffer immediate, irreparable harm if this Court denies its request for a preliminary injunction. In particular, it has shown that the Defendants—through their participation in, and operation of, the Glupteba Enterprise—have threatened the security of the internet, including Google platforms, by transmitting malware through the internet to configure, deploy, and operate a botnet. The Enterprise has distributed malware on devices of Google users, compromising the security of those devices and continues to issue commands to those devices to carry out criminal activities, such as selling access to Google user accounts and selling fraudulent credit cards to use on those accounts.

6. The Defendants control a botnet that has infected more than one million devices. At any moment, the botnet's extraordinary computing power could be harnessed for other criminal schemes. Defendants could, for example, enable large ransomware or distributed denial-of-service attacks on legitimate businesses and other targets. Defendants could themselves perpetrate such a harmful attack, or they could sell access to the botnet to a third-party for that purpose.

7. In addition, Defendants' conduct is infringing Google's trademarks, injuring Google's goodwill, and damaging its reputation by creating confusion as to the source of the Glupteba malware because the Defendants used a domain that

infringes Google's YouTube mark to distribute malware. That constitutes irreparable harm.

Likelihood of Success on the Merits

8. Google has shown at a minimum that its complaint presents a substantial question as to each of its claims, and indeed that it is likely to succeed on the merits of its claims.

9. *CFAA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the Computer Fraud and Abuse Act. The CFAA prohibits, among other things, intentionally accessing a protected computer, without authorization, and thereby obtaining information from that computer. *See* 18 U.S.C. § 1030(a)(2)(C). Defendants intentionally accessed thousands of users' computers operating in interstate commerce through the internet, without authorization, to infect them with malware. They did so to obtain information such as account credentials and URL history, which they have then sold to others. This has affected well over ten computers within a one-year span and resulted in damages significantly in excess of $5,000.

10. *ECPA*. Google has shown a likelihood of success on the merits of its claim that Defendants violated and continue to violate the Electronic Communications Privacy Act. The ECPA prohibits, among other things, "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C.

§ 2701(a). The Defendants deliberately break into the accounts of Google users and thereby obtain unauthorized access to emails and other communications stored on Google servers. They do so with the intent to acquire user credentials and other sensitive content.

11. *Lanham Act.* Google has shown a likelihood of success on the merits of its claim that Defendants violated the Lanham Act because they used Google's YouTube mark—a valid, protectable, registered and incontestable trademark—in commerce in a manner likely to cause confusion among consumers by operating a website that used the YouTube mark in the domain name and on the landing page. *See* 15 U.S.C. § 1114(1). In addition, the Lanham Act prohibits "false designations of origin" that are likely to cause confusion as to the "origin, sponsorship, or approval" of a product or service. 15 U.S.C. § 1125(a)(1)(A). It also makes unlawful a false or misleading representation, including a false designation of origin, that "in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of . . . goods, services, or commercial activities." 15 U.S.C. § 1125(a)(1)(B). The Defendants deceive internet users by falsely marketing their malware as software for downloading videos from YouTube, for their own profit, to the detriment of Google and Google's trademarks. By showing a likelihood of success on the merits of their Lanham Act claims, Google is also entitled to a presumption of irreparable harm. 15 U.S.C. § 1116(a).

12. *RICO.* Google has also shown a likelihood of success on the merits of its claims that Defendants have violated and continue to violate the RICO statute.

a. Google has shown that each Defendant is an active participant in the operation and management of the Glupteba botnet with direct ties to a C2 server previously associated with proxying activity on infected machines. Defendant Dmitry Starovikov is an administrator of Voltonwork.com. Additionally, the secondary email address for the Google Workspace Voltronwork.com account, is an email containing Dmitry's name under the Trafspin domain. Defendant Alexander Filippov is another co-conspirator who has email accounts associated with Google Workspace accounts related to Voltronwork.com, Dont.farm, and Undefined.team.

b. Google has established that Defendants have formed an enterprise. The Defendants share a common purpose to spread malware to build a botnet that is deployed for numerous criminal schemes for profit. Defendants work together to accomplish this purpose, each playing a role as described above.

c. Google has established that Defendants have engaged in a pattern of racketeering activity. The predicate acts include three separate violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A). Defendants have violated and continue to violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A), resulting in damage as defined in § 1030(c)(4)(A)(i)(VI), by infecting protected computers with malware, transmitting to such protected computers

programs designed to carry out their schemes, and transmitting to such protected computers commands to infected computers. For instance, Defendants have intentionally caused damage to "protected computers" by transmitting malware "droppers" to those computers, thereby impairing the integrity of their systems and information, and allowing Defendants to access those systems. They have also transmitted malware modules to protected computers through the internet. And they have transmitted commands to protected computers through the internet, thereby causing damage to those computers and enabling Enterprise to utilize these computers in its criminal schemes. Google is also likely to succeed on the merits of showing that the Defendants have committed predicate acts including violations of the federal wire fraud statute, 18 U.S.C. § 1343, federal identity fraud statute, 18 U.S.C. § 1028, and federal access device fraud statute, 18 U.S.C. § 1029.

d. Google has suffered injury to its business or property as a result of these predicate offenses.

13. Google has also shown a likelihood of success on the merits of its New York common law claims for tortious interference with business relationships and unjust enrichment.

Balance of the Hardships

14. The equities also favor a temporary restraining order. The criminal enterprise is defrauding consumers, and injuring Google. There is no countervailing

factor weighing against a preliminary injunction: there is no legitimate reason why Defendants should be permitted to continue to disseminate malware and manipulate infected computers to carry out criminal schemes.

Public Interest

15. Google has shown that the public interest favors granting a preliminary injunction.

16. Every day that passes, the Defendants infect new computers, steal more account information, and deceive more unsuspecting victims. Protection from malicious cyberattacks and other cybercrimes is strongly in the public interest.

17. And the public interest is clearly served by enforcing statutes designed to protect the public, such as RICO, the CFAA, the ECPA, and the Lanham Act.

PRELIMINARY INJUNCTION ORDER

IT IS HEREBY ORDERED that Defendants, any of their officers, agents, servants, employees, attorneys, and all others in active concert or participation with them, who receive actual notice of this Order by personal service or otherwise including via email ("Restrained Parties"), are restrained and enjoined from, anywhere in the world:

1. Intentionally accessing and sending malicious code to Google and the protected computers of Google's customers, without authorization;

2. Sending malicious code to configure, deploy, and operate a botnet;

3. Attacking and compromising the security of the computers and networks of Google's users;

4. Stealing and exfiltrating information from computers and computer networks;

5. Creating websites that falsely indicate that they are associated with Google, YouTube, or any other Google affiliate, through use of Google's YouTube mark and/or other false and/or misleading representations;

6. Configuring, deploying, operating, or otherwise participating in or facilitating the botnet described in the Google's moving papers, including through any component or element of the botnet in any location;

7. Delivering malicious code designed to steal credentials and cookies;

8. Monitoring the activities of Google or Google's customers and stealing information from them;

9. Selling access to the accounts of Google's customers;

10. Corrupting applications on victims' computers and networks, thereby using them to carry out the foregoing activities;

11. Offering or promoting credit cards to others for use in purchasing services from Google;

12. Misappropriating that which rightfully belongs to Google, Google's customers and users, or in which Google has a proprietary interest; and

13. Using, linking to, transferring, selling, exercising control over, or otherwise owning or accessing domains connected with the Enterprise, its activities, or its use of the botnet;

14. Using, transferring, exercising control over, or accessing any accounts used in the transfer of money or electronic currency, including cryptocurrency, or in the processing of card-based transactions, as a means to further Defendants' unlawful schemes;

15. Using and infringing Google's trademarks, including specifically Google's YouTube mark;

16. Using in connection with Defendants' activities, products or services with any false or deceptive designation, representations or descriptions of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Google or its customers or users or give Defendants an unfair competitive advantage or result in deception of consumers;

17. Acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Google, or passing off Defendants' activities, products or services as Google's; and

18. Undertaking any similar activity that inflicts harm on Google, Google's customers, or the public.

Upon service via mail, email, or text, the Defendants, and other Restrained Parties shall be deemed to have actual notice of the issuance and terms of the preliminary injunction order, and any act by any of the Restrained Parties in violation of any of the terms of the preliminary injunction order may be considered and prosecuted as contempt of Court.

IT IS FURTHER ORDERED that Google may serve this Order on the persons and entities providing services, including domain name registrars, name servers, web hosting services, and other internet service providers, relating to the domains and IP addresses identified by Google as connected to the Enterprise, its activities, or its botnet, requesting that those persons and entities take reasonable best efforts to implement the following actions:

1. Take reasonable steps to identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to such identified domains and IP addresses.

2. Take reasonable steps to block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to such identified domains and IP addresses except as explicitly provided for in this Order;

3. Take other reasonable steps to block such traffic to and/or from any other IP addresses or domains to which Defendants or Defendants' representatives moved the botnet infrastructure, to ensure that Defendants cannot use such infrastructure to control the botnet;

4. Disable completely the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with such identified domains and IP addresses and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives, and all other persons, except as otherwise ordered herein;

5. Completely, and until further order of this Court, suspend all services to Defendants or Defendants' representatives or resellers associated with such identified domains and IP addresses;

6. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives until the steps required by this Order are executed in full, except as necessary to communicate with hosting companies, data centers, Google, or other ISPs to execute this Order;

7. Not enable, and take all reasonable steps to prevent, any circumvention of this Order by Defendants or Defendants' representatives associated with such identified domains and IP addresses, including without limitation to enabling, facilitating, and/or allowing Defendants or Defendants' representatives or resellers to rent, lease, purchase, or otherwise obtain other domains and IP addresses associated with your services;

8. Preserve, retain, and produce to Google all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling such identified domains and IP addresses, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers, telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with the use of or access to such domains and IP addresses;

9. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order;

10. Completely preserve the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with such identified domains and IP addresses, and preserve all evidence of any kind related to the content, data, software or accounts associated with such domains, IP addresses, and computer hardware; and

11. IT IS FURTHER ORDERED, that in accordance with Rule 64 of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a), Plaintiff's request for an accounting of profits pursuant to 15 U.S.C. § 1117, and this Court's inherent equitable power to issue provisional remedies ancillary to its authority to provide final equitable relief, Defendants and their agents, representatives, successors or assigns, and all persons acting in concert or in participation with any of them, and any banks, savings and loan associations, credit card companies, credit card processing agencies, merchant acquiring banks, financial institutions, or other companies or agencies that engage in the processing or transfer of money and/or real or personal property, who receive actual notice of this order by personal service or otherwise, are, without prior approval of the Court, preliminarily enjoined from transferring, disposing of, or secreting any money, stocks, bonds, real or personal property, or other assets of Defendants or otherwise paying or transferring any money, stocks, bonds, real or personal property, or other assets to any of the Defendants, or into or out of any accounts associated with or utilized by any of the Defendants.

12. IT IS FURTHER ORDERED that, until further order of this Court, Google may serve this Order upon such persons as Google determines are necessary to address and enjoin activity associated with domains and IP addresses identified by Google as being used in connection with the Enterprise, its activities and its botnet, without seeking further leave of the court.

Security for Preliminary Injunction Order

IT IS FURTHER ORDERED that Google's submission of the $75,000 bond to the Clerk satisfies the requirements of this Court's temporary restraining order. See ECF 8 at 16. The Clerk is directed to accept the bond. No additional bond is necessary.

Status Report

IT IS FURTHER ORDERED that Google shall file a status report on January 31, 2022.

So ordered.

December 16, 2021

United States District Judge